**Amendments to the Claims**:

This listing of claims will replace all prior versions, and listings, of claims in the application. Please cancel claims 1-6, amend claim 7, and add claims 8-26 as follows:

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Amended) A method for efficient encryption and decryption of Internet, Intranet, or e-mail messages, comprising the steps of:

providing a sending unit in communication with an integrated encryption circuit embedded with an encryption algorithm;

encrypting a message at ~~a~~ said sending unit ~~which is to be sent to a receiving unit using an integrated circuit embedded with an algorithm located within said sending unit~~;

appending to the message at said sending unit ~~the~~ a receiver's unencrypted IP address;

appending to said message ~~the~~ a receiver's encrypted IP address;

~~said sending unit sends~~sending said encrypted message with said unencrypted IP address and said encrypted IP address to a receiving unit;

providing said receiving unit having an integrated encryption circuit embedded with a decryption algorithm;

~~receiving unit with an integrated circuit embedded with an encryption algorithm located within said~~receiving with said receiving unit said encrypted message with said unencrypted IP address and said encrypted IP address;

~~receiving unit decrypts~~decrypting with said receiving unit said encrypted IP address, thereby resulting in a decrypted IP address;~~storing said decrypted IP address in a register built into said integrated circuit embedded encryption algorithm within said receiving unit~~

storing said decrypted IP address in a first register built into said integrated encryption circuit within said receiving unit;

~~receiving unit stores~~storing said unecrypted IP address int~~o~~ a second register built into said integrated circuit ~~embedded with an encryption algorithm located~~ within said receiving unit;

means for comparing said second register storing unencrypted IP address to said first register storing said decrypted IP address;

~~receiving unit decrypts~~decrypting said message if said second register storing said unencrypted IP address matches said first register storing said decrypted ~~encrypted~~ IP address; and

means for halting decryption process if said second register storing said unencrypted IP address does not match said first register storing ~~encrypted~~said decrypted IP address.

8. (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising:

providing a communication device in communication with a private encryption key generator;

generating a primary private encryption key;

encrypting data with the primary private encryption key;

providing a public encryption key and a second private encryption key pair;

encrypting the primary private encryption key with the public encryption key and second private encryption key pair; and

sending the data encrypted with the primary private encryption key and the primary private encryption key encrypted with the public encryption key and second private encryption key pair to a receiving unit.

9. (New) The method of claim 8, wherein access to the private encryption key generator is password controlled.

10. (New) The method of claim 9 wherein the password is user defined.

11. (New) The method of claim 8 wherein said encryption key generator is located within a communication device.

12. (New) The method of claim 8 wherein the primary private key is randomly generated.

13. (New) A method of decrypting Internet, Intranet, e-mail messages, comprising:

providing a communication device in communication with a private encryption key generator;

receiving an encrypted message with the communication device, the message having data encrypted with a primary private encryption key and a primary private

encryption key encrypted with a public encryption key and second private encryption key pair;

providing access to the private encryption key generator;

decrypting the public encryption key and second private encryption key pair with the primary encryption key generator, thereby providing the primary private encryption key; and

decrypting the data with the primary private encryption key.

14. (New) The method of claim 13 wherein access to the private encryption key generator is password controlled.

15. (New) The method of claim 14 wherein the password is user defined.

16. (New) The method of claim 13 wherein access to the primary encryption key generator requires verification.

17. (New) The method of claim 16 wherein the verification comprises a Certificate of Authority.

18. (New) A method of encrypting Internet, Intranet, or e-mail messages, comprising the steps of:

providing a communication device in communication with an integrated encryption circuit embedded with encryption algorithms;

accessing the integrated encryption circuit to encrypt a message;

encrypting the message with the encryption algorithms;

providing a message header comprising the sender's private cipher key and a digital bit array;

encrypting the message header using a receiver's public encryption key;

appending the encrypted message header to the encrypted message; and

transmitting the encrypted message header and the encrypted message to a receiver.

19. (New) The method of claim 18 wherein the message is transmitted through an Internet.

20. (New) The method of claim 18 wherein the message is transmitted through an Intranet.

21. (New) The method of claim 18 wherein the message is transmitted through an e-mail.

22. (New) The method of claim 18 wherein the message is transmitted through a wireless communication system.

23. (New) A method of decrypting a message of claim 18 further comprising the steps of:

providing a communication device in communication with an integrated decryption circuit;

receiving an encrypted message and encrypted message header with the communication device;

accessing the integrated decryption circuit to decrypt the encrypted message and message header;

decrypting the message header with the decryption circuit;

validating the message header with the decryption circuit;

decrypting the message with the integrated decryption circuit; and

deleting the private cipher key from the receiver's communication device.

24. (New) An apparatus for encrypting and decrypting Internet, Intranet, and e-mail messages, comprising:

a communication device;

an integrated circuit in communication with the communication device;

a random private cipher key generator embedded within the integrated circuit;

asymmetric encryption and decryption algorithms embedded within the integrated circuit; and

symmetric encryption and decryption algorithms embedded within the integrated circuit.

25. (New) The device of claim 24 wherein the integrated circuit is capable of password protections, thereby requiring a password to access the integrated circuit.

26. (New) The device of claim 25 wherein the password is user defined.